Mr. John Mott-Smith 08 Jul 04
Director of Voting Systems
Office of the Secretary of State
1500 11th Street
Sacramento CA 95814

Subject: Certification of the Diebold Election Systems Global Election Management Systems (GEMS) Version 1-18-19, Key Card Tool Rev 1.0.1 , Voter Card Encoders (VCE) Rev 1.3.2, and AccuVote Touch Screen DRE (AV-TS R6), Firmware 4.3.15D.

Executive Summary

State certification testing was conducted 28-29 June, 2004, at the California Secretary of State Election Division offices in Sacramento, CA. for the listed revisions and new equipment: The major change are responses to the recommendations from the [Maryland] security review last year but also includes major software rewrites under the Voting Systems Standards 2002 and some minor errors noted in prior California certification testing.

The test showed significant improvement over the basic functionality and support of the voting functions and is in compliance with the California Election Code but has broadly published security weaknesses. In spite of those weaknesses, it provides better security and functional support than the currently certified version and should be adopted, with suitable Technical Security Plan procedures, to replace the current version.

References:

1. [Maryland] SAICs, *Risk Assessment Report, Diebold AccuVote-TS System and Processes* dated September 2, 2003

2. [RABA] RABA, *Trusted Agent Report Diebold AccuVote-TS Voting System* dated January 20, 2004

3. [SOS] Sate of California Secretary of State, *Certificate of Decertification and Withdrawal of Approval of Certain DRE Voting Systems and Conditional Approval of Certain DRE Voting Systems*, dated, April 30, 2004

Introduction

In compliance with California Elections Code 19200 and 19205, Diebold Election Systems applied for certification for the following revisions and new support equipment:

a. GEMS Version 1-18-19.
b. Key Card Tool Rev 1.0.1 (new)
c. Voter Card Encorders (VCE) Rev 1.3.2 (new)
d. AccuVote Touch screen Direct Record Electronic (DRE) Voting Machine, Rev 6 (AV-TS R6), Ballot Station Firmware Ver. 4.3.15D.

The AV-TS R6 and GEMS have been previously certified and used in California. This change incorporates major upgrades to the security access controls and corrects several minor errors noted in earlier versions. New or revised functionality include:

a. Secure Socket Layer/Transport Layer Security encryption support.

b. Dynamic keycard-based authentication

c. Provisions to disable and report when the Supervisor card has been permanently disabled due to invalid access attempts.

d. Consolidation of the AVServer functions into a single function (The AV-TS server was a separate function in the past with some differences in format and procedures).

Corrected errors noted in prior testing are:

1. Errors reporting write-ins in the party primary races recognizing "Decline-To-State" voters.
1. The Statement of Vote Counts (SOVC) does not correctly report the turn out data. .

NASED Qualifications

1. GEMS 1.18.19
   a. Ciber Report, dated 02-03-04 GEMS1-18-19 Final Report, A3a.pdf
   b. Ciber Report, dated 05-28-04 GEMS1-18-19 Final Report, A4a.pdf

2. Wyle Report, dated 06/04/2004, Diebold 48619-02.pdf (Change Release Report of the AccuVote-TS R6 DRE Voting Machine (Firmware Change Release 4.3.15D))

3. NASED Qualification: dated 5/20/04, N-1-06-12-12-002 (1990)
   a. GEMS 1.18.19
   b. AV-TS R6 4.3.15D
   c. Windows CE 8/8/02
   d. Spyrus Vote Card Encoder 1.3.2
   e. Key Card Utility 1.0.1

Test Report Results

The test election was based on the San Diego 2002 Primary and General with the addition of Presidential race (with semi-fictional candidates to complete General election) in seven political parties. Three parties, American Independent, Democratic, and Republican, were defined as allowing DTS voter participation and reporting with the Republican DTS not allowing Presidential. Further details are listed in the attachments.

Due to the interest and emphasis in this release of improved access controls, additional tests were completed to check the assignment of users, passwords, encryption keys, and the supervisor pin numbers. Detailed comments are provided in the attachments and summarized below.

Security Access Controls

This release of GEMS 1.18.19 and AV-TS R6 provides substantially improved security to the AV-TS R6 ballot stations. In addition to providing basic SSL/TLS to the Voter Access Card interaction and encryption to critical database files, the most visible change was to enable encryption key and supervisor Personal Identification Number (PIN) codes to be changed by the local jurisdiction election administrator. However, not all identified security weaknesses have been corrected and due caution by the local administrator is required, the results from this testing confirmed findings the RABA *Trusted Agent Report*

The following security weaknesses were noted in testing:

a. Security of the basic server and operating system is left to the local election officials who are usually untrained. Access at this level should be controlled to prevent the removal, replacement, or destruction of basic files such as GEMS, GEMS database, vote count result files, or other GEMS resources.

b. The GEMS database may be accessed by MS Access or other DAO-supported programs and modified or access gained to user access lists. (No DAO capable program other than GEMS application itself should be installed).

c. The GEMS password used to open a database in GEMS may be as small as a single letter or digit and used for all elections. (It should be a minimum of four to six characters, preferably more, and changed for each new election).

d.. SSL/TLS may be disabled for use with AV-TS R6. (Feature should always be enabled; older TS units which do not support the SSL/TLS standard should be upgraded).

e. The default encryption keys for the Smart Cards and TS internal vote counts are published openly. (Local procedures should require these to be changed before election cards are generated. The RABA report goes further and recommends that the keys be changed between precincts so that, if a key is lost in one precinct, it can not be used against the other precincts. Recording the new keys is critical to ensure later access may be reestablished should the database need to be recreated.).

f. Supervisor PINS are still defaulted to '[redacted]'. The new Key Card Tool allows the PINS to be changed but do not require it. (Local security procedures should require the PIN to be changed on installation.)

g. AV-TS R6 still restricts the PIN to four digits. Longer PINS are needed but, in their absence, the PINS may need to be changed more frequently.

h. The key locks on access panels are not secure and too easy to defeat. The panels should have seals that alert the poll workers when they check the DREs that the DRE has been tampered with.

i. The PS/2 keyboard operation is severally restricted but should be sealed off completely to eliminate the risk of access to the underlying Windows CE environment.

All of these may be countered by appropriate local procedures and checks.

Other Known Problems

The minor problem with the ballot headers on DTS ballots not displaying properly still exists but otherwise, the revision was relatively free of observed errors and problems except as noted above.

The Provisional voting resolution procedure does not support an electronic adjustment of a ballot under AB 190. Provisional ballots submitted out of the voter's registered precinct must be recreated and reprocessed as a paper provisional ballot or other appropriate manual procedure. Under the SOS Certificate of Decertification, the provisional ballots are already required to be submitted as paper ballots.

As a general observation and recommendation, GEMS shares a common condition with most of the major election management packages. The design includes features and options for other states and older election options and requirements that are inappropriate and potentially troublesome for a California election. (See for example item d in the security list).. If one of these options is enabled or not reset as appropriate and not corrected before the election is completed, the resulting election may report out incomplete or invalid results. Some systems provide a feature that allows such options to be disabled or desirable options to be automatically set based on standard requirements of the state's election code and regulations. However, Diebold does not have the capability to preset these options. I recommend that a table be added to the California procedures to provide a checklist for such options.

Conclusion

The test for this version configuration showed significant improvement over the basic functionality and support of the voting functions and is in compliance with the California Election Code but has broadly published security weaknesses. In spite of those weaknesses, it provides better security and functional support than the currently certified version and should be adopted, with suitable Technical Security Plan procedures as required in the [SOS] Certificate for Decertification an to replace the current version.

Sincerely,

Steven V. Freeman

Steven V. Freeman

Two Attachments:

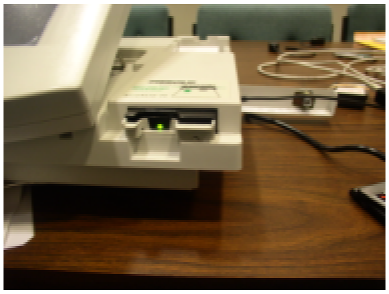
A. Hardware Description with a list of the test configuration components.
B. Test Election Design

Attachment A.

Hardware Descriptions

AccuVote-TS R6 Direct Record Electronic (DRE) Voting Machine

The AccuVote-TS R6 DRE (AV-TSR6) is a self-contained voting device consisting of a 15" LCD touch screen mounted in a unit designed to sit on a table and function as an electronic ballot station.   The touch screen display is designed to fold back against its base unit or raise to an easy viewing and voting angle during actual use. In addition to the touch screen itself, the AV-TSR6 has two PCMCIA ports, connectors for a telephone style keypad and earphone used for audio ballots, a PS/2 Keyboard connector, and a power switch located behind a locking panel door on the right hand side which locked during voting.. The panel lock uses a common key and needs to be either modified with a secure locking mechanism or provided with a tamper detection seal. A smartcard Reader/Writer is mounted on the upper right corner of the base. The DRE contains a sealed lead-acid battery and a microprocessor running Windows CE, internal thermal printer capable of printing 24 columns per line (2.25" paper width),



The device is programmed at the factory with Windows CE to support the hardware revision R6. The Ballot Station firmware which provides the general election support is installed using a special PCMCIA card inserted at power up and removed after the firmware has been updated to flash memory. The election specific database with ballot definitions are installed with another PCMCIA card which left resident in the DRE to record results. There is currently no capability to transfer the results directly to the PC. The PCMCIA cards must be consolidated or installed in an AV-TS R6 that is connected to the PC and transferred electronically from the forwarding DRE to the PC. The protocol of the electronic transfer has been proven to be vulnerable to interception so the cable connection should be restricted to short distances where the connection is under observation at all times. Vote totals are also stored independently in memory and can be recovered after the election as an independent record but again must be transferred via a DRE.

Voter Access Components: Key Card Tool and Voter Card Encoder (VCE)

Identification of authorized access is through access smartcards. Two forms of access are allowed: supervisor (bottom card in picture below) and voter (middle card). Both forms use Secure Socket Layer/Transport Layer Security (SSL/TLS) protocols to provide secure access. The cards have encrypted electronic signatures to verify the card and the integrity of its contents. Additional information is recorded on the card to identify the user's access rights to specific ballots (Voter) or functions (Supervisor).

The new functionality provides for a special card called the Master Key card. The Key Card Tool, a software utility which is installed in a PC with compatible PCMCIA card reader/writer, allows the local election official to change the encryption keys used by the smartcards and the DRE as well as the authorization Pin number required to authenticate Supervisor access. The Key Card Tool creates a Master Key card that identifies the old key (to authenticate it when the keys are transferred) and the new keys or pin. The Master Key card is used to change the keys and/or supervisor pin numbers on the DREs before the election. The Key Card Tool is also used to update the Supervisor cards with new pin numbers.

Critical: the election official must record and keep secure the new smartcard key once created as it will be needed to program/change the other keys and to create new Supervisor cards.

The Voter Card Encorder (VCE) (top item in the picture) is a Spyrus smart card reader/writer, a commercial product, which is preset by Diebold for use as a VCE. Each VCE can store and program Voter Access cards for eight ballot ids. The device is programmed using a voter access card to transfer the voter ids from a DRE which has been programmed for the election. The eight ballot ids may be for eight precincts, eight primary parties with their own ballot id, or combinations of both up to the maximum of eight ballot ids. For the primary test election used in this primary, there were 11 ballot ids within each precinct so it would take a minimum of two VCEs per precinct to generate voter access cards for that precinct.

Test Configuration Inventory

1. Dell Power Edge 600SC, HH18021 Chassis S/N
    a. 1.8 gigahertz, Pentium 4 processor
    b. 1 MByte RAM
    c. 20 GByte IDE Internal Hard Drive
    d. PLEXTOR CD-R PX-W1210S SCSI CdRom Drive
    e. 3.5 Diskette Drive
    f. ARCHIVE Python 06408-XXX SCSI Sequential Tape Drive (not used)

Note: after encountering problems with the CdRom Drive, two USB drives were used to upload installation software and download archive results.

    g. USB Hard Drive 20 GByte
    h. Sandisk Attaché Thumb drive 128KByte

2. Commercial-Off-The-Shelf Software
    a. MS Windows 2000 Server, Service Pack 4
        i. Window Internet Explorer 6.00.2800.1106
    b. Adobe Acrobat Version 6.0.0.2003051900
    c. Nero CD/DVD Rom Burning Suite, Version 6,
    d. WinZip 8.1, SR1

Note: All the above were installed using commercial installation sets on a clean system. Some additional packages were installed such as the Kodak picture utilities as included in the MS Windows 2000 install but are not germaine to this test

e. Crystal Reports. Loaded by the GEMS application as part of its install.

3. Three AccuVote TS-R6, Ballot Station 4.3.15D
   a. S/N 159084
   b. S/N 159114
   c. S/N 159519, used for voter card programming.
4. Three Spyrus Voter Card Encoders

Attachment B.

Test Election Design

	Precinct	1	2	2	3	4	5	6	7	8	9	10
Type	**Split**		1	2								
SW	Federal, STATE	x	x	x	x	x	x	x	x	x	x	x
SD	Board of Equal 3	x	x	x	x	x	x	x	x	x	x	x
SD	CONGRESS 49	x	x	x								
SD	CONGRESS 50				x	x						
SD	CONGRESS 51						x	x				
SD	CONGRESS 52								x	x		
SD	CONGRESS 53										x	x
SD	STATE SENATE 36	x	x									
SD	STATE SENATE 37				x		x					
SD	STATE SENATE 38			x		x						
SD	STATE SENATE 39								x		x	
SD	STATE SENATE 40							x		x		x
SD	ASSEMBLY 66	x							x			
SD	ASSEMBLY 74				x					x		
SD	ASSEMBLY 75		x	x							x	
SD	ASSEMBLY 76						x	x				
SD	ASSEMBLY 77					x						x
U	COUNTY, Unincorporated		x					x				
C	CHULA VISTA			x								
C	LEMON GROVE	x										
R	PORTER VISTA					x						
S	Measure	x	x	x	x	x	x	x	x	x	x	x

C city, M Military, R unincorporated remainder of county, U Unincorporated place in a county.

Further details on test election makeup and

The test election was modified from the San Diego by combining various districts and races into a selection of ten precincts which concisely included samples of state, statewide district (State Senate and Assembly Districts), judicial, (See Test Design Matrix above). Only first five precincts with one split precinct were used in this test due to testing time limits but these are adequate to test all but the supervisor district rotations.

Since this was a DRE, all test voting was done manually directly into two of the three DREs. Volume testing with millions of votes is performed by Wyle Labs, the hardware ITA. Our test emphasized more direct voter actions.

The third DRE was setup to support reprogramming Voter Card Encoder devices (VCE) but the actual Voter Access Cards were programmed from an actual VCE. Because of the limit of eight ballot ids per VCE, we had to reprogram the VCE to recognize all five precincts and combinations of parties within the five tested precincts.   One round of votes were counted as absentee/early voting while a second round were counted as polling place ballots to exercise consolidation of the ballot counts for the two types of voting on GEMS. Also, write-ins and provisional ballots were included to test the recording and reconciliation of write-ins and provisional ballots.

A total of 130 ballots were cast. exercising the following ballot logic and conditions:

1. Primary party ballots with DTS voting and reporting
2. Non-Partisan races
3. Split precinct
4. Vote for 2 of 5,
5. Write-in votes (including potential over-vote conditions)
6. Blank ballots
7. Provisional ballots
8. Rotation based on assembly district at state, state districts, and local levels
9. Multiple languages (English, Spanish, and Vietnamese)
    a. Wyle ITA testing tested for all seven in use in California)
10. Long names in candidate fields.
11. Turn-out statistics on final summary reports
12. Measures
13. Touch screen navigation between contests and return from the review screen provided before finally casting ballots.
14. Glides, double taps, and other voter touch screen responses that can result in skipping races or pre-mature casting of ballot
15. Audio ballots in three languages.
16. Power interruptions
17. Polls open, close, and report printing.
18. Review of audit logs.